Serial No.: 10/575,158

## 1 LISTING OF THE CLAIMS 2 **CLAIMS** 3 1. (Currently amended) A method for attestation comprising generating a user 4 attestation-signature value for use with a verification computer, the user attestation-signature 5 value corresponding to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, 6 z), none, one, or more of the attribute values (w, y) remaining anonymous for transactions 7 performable by a user device having a security module with the verification computer, the step of 8 generating comprising the steps of: 9 - providing a user public key and a proof value that demonstrates that the user public key was 10 validly derived from a module public key of the security module; 11 - receiving from an attester computer: 12 (I) an attestation value having the at least one attribute (A, B, C, D) with its attribute value (w, x, y, z), none, one or more of the attribute values (x, y) remaining unknown to 13 14 the attester computer, 15 the attestation value being derived from an attester secret key, a user public key, 16 and none, one, or more attester determined attribute values (w, z), 17 the user public key inherently comprising none, one, or more user determined 18 attribute values (x, y), and 19 (II) at least one of the attester determined attribute values (w, z); and - deriving the user attestation-signature value from the attestation value and a security module

attestation value provided by the security module,

20

21

Serial No.: 10/575,158

1	wherein:
-	Willer Cill.

2	it is verifiable whether or not (i) the user attestation-signature value was validly derived
3	from the security module attestation value and the attestation value, and that (ii) the attestation
4	value is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D)
5	having a revealed attribute value (x, z);
6	the step of deriving the user attestation-signature value further comprises the steps of:
7	receiving from the security module a first security module attestation value,
8	deriving an intermediate user attestation-signature value from the first security module
9	attestation value under use of an attester public key and a hash function;
10 11	providing the intermediate user attestation-signature value to the security module, receiving from the security module a part of the user attestation-signature value, and
11	receiving nem the security medical a part of the deer attended bighatare value, and
12	calculating by the user device further parts of the user attestation-signature value using
13	none, one, or more of the attribute values (w, y), the received part of the user
14	attestation-signature value, the user public key, and the attester public key;
15 16	the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values (x, y);
17	the user device provides encryptions under a trusted third party's public key of one or
18	more of the attribute values (w, y) that remain unknown to the verification computer;
19 20	the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values $(x, y)$ ;

Serial No.: 10/575,158

1	the user deviceprovides encryptions under a trusted third party's public key of one or
2	more of the attribute values (w, y) that remain unknown to the verification computer;
3	the user device provides encryptions under a trusted third party's public key of one or
4	more of the attribute values (w, y) that remain unknown to the verification computer;
5	the step of deriving the user attestation-signature valuefurther comprises the steps of:
6	receiving from the security module a first security module attestation value,
7	deriving an intermediate user attestation-signature value from the first security module
8	attestation value under use of an attester public key and a hash function,
9	providing the intermediate user attestation-signature value to the security module;
10	receiving from the security module a part of the user attestation-signature value, and
11	calculating by the user device further parts of the user attestation-signature value using
12	none, one, or more of the attribute values (w, y), the received part of the user
13	attestation-signature value, the user public key, and the attester public key; and
14	the user public key is derived from the module public key by using the attester public key
15	and the one or more of the attribute values $(x, y)$ ; and
16	the user device provides encryptions under a trusted third party's public key of one or
17	more of the attribute values (w, y) that remain unknown to the verification computer.
18 19	2 20. (Canceled)